10/510606
PCT/FR03/01169

R E P U B L I Q U E F R A N Ç A I S E

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 09 JUIL. 2003

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

DOCUMENT DE PRIORITÉ

PRÉSENTÉ OU TRANSMIS CONFORMÉMENT À LA RÈGLE 17.1.a) OU b)

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr

ETABLISSEMENT PUBLIC NATIONAL CREE PAR LA LOI N° 51-444 DU 19 AVRIL 1951

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

refra N° 11354*01

REQUÊTE EN DÉLIVRANCE 1/2

Important ! Remplir impérativement la 2ème page.

Cet imprimé est à remplir lisiblement à l'encre noire DB 540 W /190600

Réservé à l'INPI

REMISE DES PIÈCES
DATE
LIEU 12 AVR. 2002
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0204840
DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI 12 AVR. 2002

Vos références pour ce dossier *(facultatif)* PF020035

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

THOMSON multimedia
European Patent Operations
46 quai A. Le Gallo
92648 Boulogne Cedex

A l'attention de Karine BERTHIER

Confirmation d'un dépôt par télécopie ☒ N° attribué par l'INPI à la télécopie 1283

2 NATURE DE LA DEMANDE	Cochez l'une des 4 cases suivantes
Demande de brevet	☒
Demande de certificat d'utilité	☐
Demande divisionnaire	☐
Demande de brevet initiale	N° Date
ou demande de certifical d'utilité initiale	N° Date
Transformation d'une demande de brevet européen *Demande de brevet initiale*	☐ N° Date

3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)

PROCEDE D'AUTHENTIFICATION ANONYME D'UN EMETTEUR DE DONNEES

4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE	Pays ou organisation Date N°
	Pays ou organisation Date N°
	Pays ou organisation Date N°
	☐ **S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»**
5 DEMANDEUR	☐ **S'il y a d'autres demandeurs, cochez la case et utilisez l'imprimé «Suite»**
Nom ou dénomination sociale	THOMSON LICENSING S.A.
Prénoms	
Forme juridique	S.A.
N° SIREN	3 8 3 4 6 1 1 9 1
Code APE-NAF	3 2 2 A
Adresse — Rue	46 Quai Alphonse Le Gallo
Adresse — Code postal et ville	92648 Boulogne cedex
Pays	FRANCE
Nationalité	Française
N° de téléphone *(facultatif)*	01 41 86 54 88
N° de télécopie *(facultatif)*	01 41 86 56 34
Adresse électronique *(facultatif)*	berthierk@thmulti.com

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

REQUÊTE EN DÉLIVRANCE 2/2

Réservé à l'INPI

REMISE DES PIÈCES DATE LIEU	12 AVR. 2002
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI	0204840

DB 540 W /190600

Vos références pour ce dossier : *(facultatif)*		PF020035
6 MANDATAIRE		
Nom		BERTHIER
Prénom		Karine
Cabinet ou Société		THOMSON multimedia
N °de pouvoir permanent et/ou de lien contractuel		9016
Adresse	Rue	46 Quai Alphonse Le Gallo
	Code postal et ville	92648 Boulogne cedex
N° de téléphone *(facultatif)*		01 41 86 54 88
N° de télécopie *(facultatif)*		01 41 86 56 34
Adresse électronique *(facultatif)*		berthierk@thmulti.com
7 INVENTEUR (S)		
Les inventeurs sont les demandeurs		☐ Oui ☒ Non **Dans ce cas fournir une désignation d'inventeur(s) séparée**
8 RAPPORT DE RECHERCHE		**Uniquement pour une demande de brevet (y compris division et transformation)**
Établissement immédiat ou établissement différé		☐ ☐
Paiement échelonné de la redevance		**Paiement en deux versements, uniquement pour les personnes physiques** ☐ Oui ☐ Non
9 RÉDUCTION DU TAUX DES REDEVANCES		**Uniquement pour les personnes physiques** ☐ Requise pour la première fois pour cette invention *(joindre un avis de non-imposition)* ☐ Requise antérieurement à ce dépôt *(joindre une copie de la décision d'admission pour cette invention ou indiquer sa référence)* :
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes		

10 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE
(Nom et qualité du signataire)
BERTHIER Karine
Mandataire

VISA DE LA PRÉFECTURE OU DE L'INPI

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire.
Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

La présente invention concerne l'échange sécurisé de données à travers un réseau reliant différents dispositifs et l'authentification de la source de données émises sur un réseau.

Dans certains cas, il est nécessaire pour un dispositif récepteur de données d'être sûr que l'émetteur qui a diffusé les données était bien autorisé à le faire par un tiers de confiance sans que le récepteur des données ne connaisse l'identité de l'émetteur, les données étant également susceptibles d'être relayées par un dispositif intermédiaire. Or tous les schémas connus d'authentification d'un émetteur de données impliquent que le récepteur des données connaisse l'émetteur.

Un but de l'invention est donc de proposer une méthode permettant à un émetteur de données de prouver qu'il était bien autorisé à émettre les données par un tiers de confiance sans que le récepteur des données ne connaisse l'identité de l'émetteur.

A cet effet, l'invention a pour objet un procédé permettant de vérifier que des données reçues par un récepteur ont été envoyées par un émetteur autorisé par un tiers de confiance, l'émetteur et le récepteur étant raccordés à un réseau numérique. Selon l'invention, un identifiant est associé aux données envoyées par l'émetteur et le procédé comprend les étapes consistant, pour le récepteur, à :

- générer un nombre aléatoire ;
- diffuser sur le réseau ledit nombre aléatoire ;
- recevoir de l'émetteur une réponse calculée en appliquant une première fonction audit nombre aléatoire et audit identifiant ; et
- vérifier la réponse reçue en appliquant une seconde fonction à la réponse reçue, audit nombre aléatoire et audit identifiant ;

la première fonction ayant été au préalable délivrée à l'émetteur par le tiers de confiance et la seconde fonction étant une fonction booléenne, liée à la première fonction, délivrée au préalable par le tiers de confiance au récepteur.

L'émetteur peut être soit l'émetteur initial des données dans le réseau, soit un intermédiaire entre l'émetteur initial et le récepteur des données qui a par exemple stocké les données émises par l'émetteur initial.

L'identifiant associé aux données envoyées par l'émetteur est préférentiellement un nombre aléatoire généré par l'émetteur initial des

données dans le réseau et attaché à ces données par l'émetteur initial. Bien entendu, cet identifiant ne donne aucune information sur l'identité de l'émetteur.

Selon le principe de l'invention, un tiers de confiance délivre à tous les dispositifs susceptibles d'être des émetteurs initiaux ou intermédiaires dans un réseau, la première fonction permettant de calculer la réponse dans le cadre du procédé ci-dessus. Le tiers de confiance délivre également à tous les dispositifs susceptibles d'être des récepteurs dans le réseau, le seconde fonction permettant de vérifier la réponse calculée à l'aide de la première fonction.

L'invention sera mieux comprise à la lecture de la description qui va suivre, donnée uniquement à titre d'exemple et faite en se référant à la figure unique (Fig. 1) qui représente un réseau numérique domestique dans lequel est mise en œuvre l'invention.

Sur la base du principe de l'invention exposé ci-dessus, plusieurs scénarios sont possibles.

Selon un premier scénario, un premier émetteur, que nous appellerons Alice, et un second émetteur, que nous appellerons Charlie, diffusent des messages respectivement appelés M_A et M_C sur un réseau auquel est raccordé un récepteur, que nous appellerons Bob. Alice diffuse avec le message M_A un identifiant $IdEvent_A$ qui identifie le message M_A et Charlie diffuse avec le message M_C un identifiant $IdEvent_C$ qui identifie le message M_C.

Alice et Charlie qui sont tous deux raccordés au réseau reçoivent respectivement les messages M_C et M_A émis par l'autre émetteur du réseau mais ils ne les conservent pas. Bob reçoit également les deux messages et nous supposons qu'il ne souhaite conserver que le message M_A. Pour être sûr que M_A provient d'une source autorisée par un tiers de confiance, Bob lance un protocole challenge/réponse de la manière suivante. Bob génère un nombre aléatoire C (le challenge) puis il le diffuse sur le réseau. Alice et Charlie reçoivent tous deux le challenge C.

Au préalable, nous supposons que le tiers de confiance a délivré à Alice et Charlie une fonction G de calcul de réponse et a délivré à Bob une fonction H correspondante de vérification de réponse.

Lorsque Alice et Charlie reçoivent le challenge C émis par Bob, ils calculent respectivement des réponses R_A et R_C comme suit :

Alice : $R_A = G(IdEvent_A, C)$;

Charlie : $R_C = G(IdEvent_C, C)$;

puis ils envoient les réponses R_A et R_C à Bob.

Bob vérifie ensuite chaque réponse en calculant $H(C, R_X, IdEvent_A)$ pour X = A et C. Si tous les résultats retournés par la fonction H sont nuls, alors Bob ne conserve pas le message M_A qui est considéré comme ne provenant pas d'une source sûre. Par contre, si au moins un résultat retourné par H est égal à 1 (dans l'exemple, il s'agira de $H(C, R_A, IdEvent_A)$), alors Bob accepte le message M_A car il est assuré qu'il provient d'un émetteur autorisé par le tiers de confiance.

Selon un second scénario, un émetteur, Alice, diffuse un message M_A accompagné d'un identifiant $IdEvent_A$ sur un réseau auquel est raccordé un récepteur Bob et une entité intermédiaire, que nous appellerons Déborah. Nous supposons que Bob n'est pas intéressé par le message M_A et qu'il ne le conserve pas. Déborah par contre enregistre le message M_A et son identifiant $IdEvent_A$.

Plus tard, alors qu'Alice ne diffuse plus de message, nous supposons que Déborah diffuse le message M_A enregistré et son identifiant $IdEvent_A$ sur le réseau. Alice étant seulement un émetteur ne conserve pas M_A. Bob reçoit M_A et souhaite le conserver. Pour s'assurer qu'il provient d'une source autorisée par un tiers de confiance, Bob lance un protocole challenge/réponse de la manière suivante. Bob génère un nombre aléatoire C (le challenge) puis il le diffuse sur le réseau.

Au préalable, nous supposons que le tiers de confiance a délivré à Alice et Déborah une fonction G de calcul de réponse et a délivré à Bob une fonction H correspondante de vérification de réponse.

Alice et Déborah reçoivent le challenge C. Comme Alice n'est pas en train de diffuser un message, elle ne tient pas compte du challenge C. Déborah par contre calcule une réponse $R_D = G(IdEvent_A, C)$ et envoie cette réponse à Bob. Bob vérifie ensuite cette réponse en calculant $H(C, R_D, IdEvent_A)$. Si la fonction H retourne 0, alors Bob ne conserve pas le message M_A. En revanche, si la fonction H retourne 1, alors Bob accepte le message M_A qui est considéré comme provenant d'une source autorisée.

On notera que dans les deux scénarios exposés ci-dessus, l'entité récepteur Bob ne sait pas si le message qu'il reçoit provient d'un émetteur (comme Alice) ou d'un intermédiaire (comme Déborah) et surtout il ne connaît pas l'identité du diffuseur du message M_A.

Nous allons maintenant décrire un exemple plus concret de mise en œuvre de l'invention en référence à la figure 1 où sont représentés un décodeur STB (de l'anglais « Set Top Box ») 1, un récepteur de télévision numérique DTV (de l'anglais « Digital Television ») 2 et un dispositif d'enregistrement SU (de l'anglais « Storage Unit ») 3.

Nous supposons que les données diffusées sur ce réseau représentent des programmes audiovisuels composés de flux élémentaires Audio et Vidéo transportés dans un flux de transport de données tel que défini dans la norme ISO/IEC 13818-1 « *Information technology – Generic coding of moving pictures and associated audio information : Systems* ».

Le décodeur 1 représente un émetteur de données sur le réseau, il émet des données qu'il reçoit par exemple d'une antenne satellite ou d'une connexion au câble. Le téléviseur numérique 2 représente un récepteur de données sur le réseau. Le dispositif d'enregistrement 3 représente quant à lui un dispositif intermédiaire capable de rediffuser sur le réseau des données reçues d'un autre dispositif émetteur du réseau.

Ces trois dispositifs sont raccordés à un bus numérique 4, par exemple un bus selon la norme IEEE 1394, et forment ainsi un réseau domestique numérique. Les messages diffusés dans le réseau sont envoyés à travers le canal isochrone du bus 4 et les messages qui sont adressés sont envoyés à travers le canal asynchrone du bus 4.

Le tiers de confiance qui délivre une fonction G de calcul de réponse à un protocole challenge/réponse aux dispositifs émetteurs ou intermédiaires du réseau (dans notre exemple, le décodeur 1 et le dispositif d'enregistrement 3) et qui délivre une fonction H de vérification de réponse aux dispositifs récepteurs du réseau (dans notre exemple le téléviseur numérique 2) est par exemple le fabriquant des dispositifs.

En ce qui concerne le choix des fonctions G et H, nous envisagerons trois modes de réalisation.

Selon un premier mode de réalisation préféré, la fonction G est une fonction publique qui utilise une clé secrète K pour calculer une réponse R à partir d'un challenge C et d'un identifiant IdEvent (i.e. $R = G_K(C, IdEvent)$). Pour garantir que les dispositifs émetteurs ou intermédiaires sont des appareils conformes, autorisés par le tiers de confiance, le secret K est inséré dans ces dispositifs, dans une zone de stockage sécurisée qui ne doit plus être accessible ultérieurement (par exemple dans un processeur sécurisé, notamment inclus dans une carte à puce).

La fonction H est dans ce cas une fonction qui calcule une réponse R' à partir du challenge C et de l'identifiant IdEvent en appliquant la fonction G avec la clé secrète K et qui compare ensuite le résultat R' avec la réponse R reçue. H est une fonction booléenne qui délivre une valeur nulle « 0 » si R' est différent de R et qui délivre une valeur « 1 » si R' est égal à R. Dans ce cas, la clé secrète K doit aussi être insérée au préalable par le tiers de confiance dans les dispositifs récepteurs.

Une fonction G correspondant à la définition ci-dessus peut être notamment une fonction de chiffrement telle que la fonction AES décrite notamment dans « *FIPS 197 : Specification of the Advanced Encryption Standard (AES) –26 novembre 2001* » disponible à l'adresse Internet suivante : *http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.* Il peut également s'agir d'une fonction de hachage telle que la fonction HMAC-SHA1 décrite notamment dans « RFC 2104 : HMAC : Keyed-Hashing for Message Authentication – Fevrier 1997 » disponible à l'adresse Internet suivante : *http://www.ietf.org/rfc/rfc2104.txt.*

Dans un second mode de réalisation, la fonction G est une fonction secrète qui est insérée dans les dispositifs émetteurs ou intermédiaires considérés comme conformes et autorisés par le tiers de confiance. Préférentiellement, cette fonction doit être choisie de manière à être très difficilement retrouvée par l'analyse des produits qui la contiennent. De plus cette fonction doit être résistante aux attaques à texte clair choisi adaptatives (plus connues sous le nom anglais de « adaptive chosen-plaintext attacks »).

De même que dans le premier mode de réalisation, la fonction H est dans ce cas une fonction booléenne qui calcule une réponse R' à partir du challenge C et de l'identifiant IdEvent en appliquant la fonction G secrète et qui compare ensuite le résultat R' avec la réponse R reçue, délivrant une valeur nulle « 0 » si R' est différent de R et délivrant une valeur « 1 » si R' est égal à R. Dans ce mode de réalisation, la fonction secrète G doit donc aussi être insérée au préalable par le tiers de confiance dans les dispositifs récepteurs.

Dans un troisième mode de réalisation, les fonctions G et H sont des fonctions publiques utilisant une paire de clés asymétrique (clé privée/clé publique). La fonction G est par exemple une fonction de génération de signature à l'aide d'une clé privée et la fonction H est une fonction de vérification de signature à l'aide d'une clé publique correspondante.

Nous utiliserons par exemple les fonctions de signature RSA (acronyme du nom des créateurs Rivest, Shamir et Adleman) comme suit :

$R = G(C, IdEvent) = RSASign_{KPRIV}(C, IdEvent)$ et

$H(C, R, IdEvent) = RSAVerif_{KPUB}(C, R, IdEvent)$; où KPRI et KPUB sont la clé privée et la clé publique d'une même paire de clé RSA.

Dans ce cas, la clé privée est insérée dans les dispositifs émetteurs ou intermédiaires du réseau par le tiers de confiance et la clé publique est insérée dans les dispositifs récepteurs du réseau.

Nous supposerons dans la suite que le premier mode de réalisation a été choisi dans lequel la fonction G est la fonction HMAC-SHA1 et qu'une clé secrète K est incluse dans une zone de stockage inviolable du décodeur STB 1, du récepteur de télévision numérique DTV 2 et du dispositif d'enregistrement SU 3.

Premier scénario : le STB transmet directement un programme au DTV

Lorsque l'utilisateur du décodeur STB 1 sélectionne un nouveau programme pour qu'il soit diffusé dans le réseau, le STB génère aléatoirement un identifiant de programme IdEvent, qui est préférentiellement un nombre de 128 bits et il insère cet identifiant dans des messages contenus dans les paquets de transport des données représentant le programme. Le flux de transport de données est ensuite diffusé sur le réseau (sur le canal isochrone du bus 4). Il est reçu par le téléviseur numérique DTV 2 qui extrait des paquets de données reçus les messages contenant l'identifiant pour récupérer cet identifiant IdEvent.

Le DTV génère alors un challenge C, qui est préférentiellement un nombre aléatoire de 128 bits, et il diffuse ce challenge C sur le réseau. Lorsque le STB reçoit le challenge C, il calcule la réponse :

$R_{STB} = HMAC\text{-}SHA1_K(C, IdEvent)$

et adresse cette réponse au DTV par le canal asynchrone du bus 4.

Le dispositif d'enregistrement SU 3, qui reçoit également le challenge C ne répond pas puisqu'il n'est pas en train de diffuser des données.

Lorsque le DTV reçoit la réponse R_{STB} du STB, il calcule :

$R_{DTV} = HMAC\text{-}SHA1_K(C, IdEvent)$ et compare ce résultat à la réponse R_{STB} reçue. Si les deux valeurs sont les mêmes, alors le DTV

considère que le programme reçu provient d'un émetteur autorisé par le tiers de confiance. Sinon, le DTV n'affiche pas à l'utilisateur le programme reçu.

A la fin du protocole, le challenge C et l'identifiant IdEvent sont effacés des mémoires du STB et du DTV.

Second scénario : le STB transmet un programme qui est stocké par le SU qui le diffuse ultérieurement au DTV.

Dans un premier temps, on suppose que l'utilisateur du STB sélectionne un nouveau programme. Le STB génère alors un identifiant IdEvent comme dans le premier scénario ci-dessus et il insère cet identifiant dans des messages inclus dans les paquets de transport des données représentant le programme avant de diffuser le flux de transport de données sur le réseau.

Le SU enregistre ensuite le flux de données représentant le programme. L'utilisateur a par exemple choisi de ne pas visualiser tout de suite le programme qui est diffusé par le décodeur et préfère l'enregistrer pour le relire plus tard.

Dans un deuxième temps, l'utilisateur souhaite relire le programme enregistré. Le SU diffuse donc le programme sur le réseau. Le DTV reçoit les paquets de données et en extrait les messages contenant l'identifiant IdEvent.

Le DTV génère ensuite un challenge C comme dans le premier scénario et il diffuse ce challenge sur le réseau.

Le SU reçoit ce challenge C, il calcule donc la réponse :

R_{SU} = HMAC-SHA1$_K$(C, IdEvent)

et adresse cette réponse au DTV par le canal asynchrone du bus 4.

Le STB qui n'est pas en train de diffuser des données ne répond pas au challenge C qu'il reçoit également.

Lorsque le DTV reçoit la réponse R_{SU} du SU, il calcule :

R_{DTV} = HMAC-SHA1$_K$(C, IdEvent) et compare ce résultat à la réponse R_{SU} reçue. Si les deux valeurs sont les mêmes, alors le DTV considère que le programme reçu provient d'un émetteur autorisé par le tiers de confiance. Sinon, le DTV n'affiche pas à l'utilisateur le programme reçu.

On notera que lorsque le STB a terminé de diffuser le programme dans le premier temps, il efface ensuite l'identifiant IdEvent de sa mémoire.

A la fin du protocole, le challenge C et l'identifiant IdEvent sont également effacés des mémoires du SU et du DTV.

L'invention présente notamment les avantages suivants :

Même si plusieurs dispositifs émetteurs ou intermédiaires sont raccordés au réseau, seul celui qui a été autorisé par le tiers de confiance et qui a émis les données est capable de répondre au protocole challenge/réponse initié par le récepteur des données.

Le protocole ne divulgue aucune information concernant l'émetteur au récepteur. Ceci permet d'atteindre l'objectif d'une authentification anonyme du dispositif émetteur.

Le protocole repose uniquement que la couche application et ne requiert aucune particularité au niveau de la couche transport des données.

REVENDICATIONS

1. Procédé pour vérifier que des données reçues par un récepteur ( ) ont été envoyées par un émetteur ( ) autorisé par un tiers de confiance, l'émetteur et le récepteur étant raccordés à un réseau numérique, caractérisé en ce qu'un identifiant (IdEvent) est associé aux données envoyées par l'émetteur et en ce que le procédé comprend les étapes consistant, pour le récepteur (), à :

- générer un nombre aléatoire (C) ;
- diffuser sur le réseau ledit nombre aléatoire ;
- recevoir de l'émetteur une réponse (R) calculée en appliquant une première fonction (G) audit nombre aléatoire (C) et audit identifiant (IdEvent) ;
- vérifier la réponse (R) reçue en appliquant une seconde fonction (H) à la réponse reçue (R), audit nombre aléatoire (C) et audit identifiant (IdEvent) ;

la première fonction (G) ayant été au préalable délivrée à l'émetteur par le tiers de confiance et la seconde fonction (H) étant une fonction booléenne, liée à la première fonction, délivrée au préalable par le tiers de confiance au récepteur.

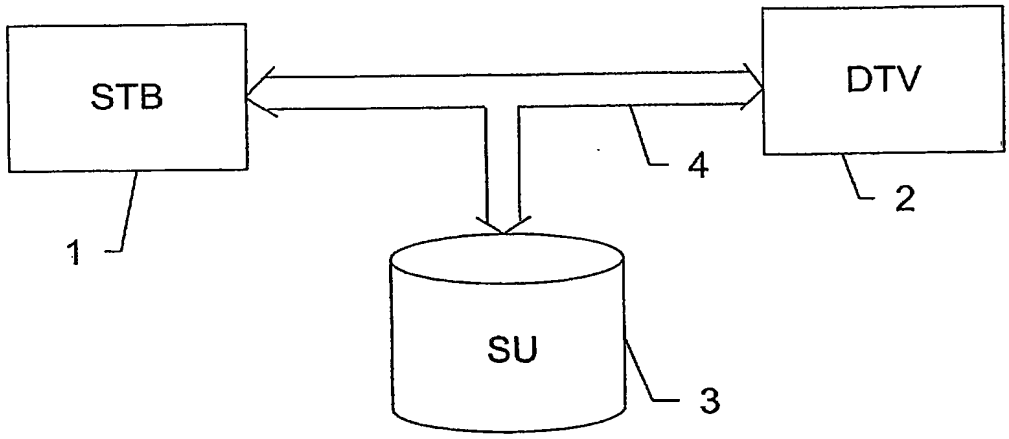


Fig. 1

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11235*02

DÉSIGNATION D'INVENTEUR(S) Page N° 1. / 1.
(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)

Cet imprimé est à remplir lisiblement à l'encre noire — DB 113 W /260899

Vos références pour ce dossier *(facultatif)*	PF020035
N° D'ENREGISTREMENT NATIONAL	0204840

TITRE DE L'INVENTION (200 caractères ou espaces maximum)
PROCEDE D'AUTHENTIFICATION ANONYME D'UN EMETTEUR DE DONNEES

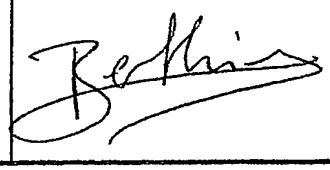
LE(S) DEMANDEUR(S) :
THOMSON LICENSING S.A.
46 Quai Alphonse Le Gallo
92648 Boulogne cedex
FRANCE

DESIGNE(NT) EN TANT QU'INVENTEUR(S) : (Indiquez en haut à droite «Page N° 1/1» S'il y a plus de trois inventeurs, utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages).

Nom		DIEHL	
Prénoms		Eric	
Adresse	Rue	La Buzardière	
	Code postal et ville	35340	Liffré
Société d'appartenance *(facultatif)*			
Nom		ANDREAUX	
Prénoms		Jean-Pierre	
Adresse	Rue	20 rue de Lorgenil	
	Code postal et ville	35000	Rennes
Société d'appartenance *(facultatif)*			
Nom		DURAND	
Prénoms		Alain	
Adresse	Rue	79, rue de Dinan	
	Code postal et ville	35000	Rennes
Société d'appartenance *(facultatif)*			

DATE ET SIGNATURE(S)
DU (DES) DEMANDEUR(S)
OU DU MANDATAIRE
(Nom et qualité du signataire)

BERTHIER Karine
Mandataire



La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☑ BLACK BORDERS
- ☑ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☑ FADED TEXT OR DRAWING
- ☑ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☑ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☑ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.